REMARKS

This Amendment and Response to Non-Final Office Action is being submitted in response to the non-final Office Action mailed August 10, 2007. Claims 1-38 are pending in the Application.

Claims 33-37 are rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 1-38 are rejected under 35 U.S.C. §103(a) as being unpatentable over Sharma *et al.* (U.S. Pat. No. 6,766,165) in view of Heitman *et al.* (U.S. Pat. No. 6,920,494).

In response to these rejections, Claims 1, 14, 29, and 33-38 have been amended to further clarify the subject matter which Applicants regard as the invention, without prejudice or disclaimer to continued examination on the merits. These amendments are fully supported in the Specification, Drawings, and Claims of the Application and no new matter has been added. Based upon the amendments and the arguments presented herein, reconsideration of the Application is respectfully requested.

Information Disclosure Statement

Examiner requests Applicants stipulate as to each and every reference cities on the IDS submitted on 3/4/2004 which is material to patentability. Applicants respectfully submit the information required to be submitted is unknown and/or is not readily available to the party or parties from which it was requested. See M.P.E.P. §704.12(b). Additionally, M.P.E.P. §704.12(a) states "similar to 37 CFR 1.56, applicant is required by 37 CFR 1.105 to submit information already known, but there is no requirement to search for information that is unknown."

Claims 33-37 - §112, Second Paragraph, Rejection

Claims 33-37 are rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Examiner states that "node/node relationship" is unclear. In response to this rejection, Applicant has amended Claims 33 and 36 to change access point/node to access point to node and node/node to node to node. Accordingly, Applicant respectfully submits that the rejection of Claims 33-37 as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention has been traversed, and respectfully requests withdrawal of this rejection.

Claims 1-38 - §103(a) Rejection – Sharma *et al.*, Heitman *et al.*

Claims 1-38 are rejected under 35 U.S.C. §103(a) as being unpatentable over Sharma *et al.* (U.S. Pat. No. 6,766,165) in view of Heitman *et al.* (U.S. Pat. No. 6,920,494). In response to this rejection, Applicant has amended Claims 1, 14, 29, and 33-38.

With regard to Claim 1, Sharma *et al.* and Heitman *et al.* do not teach receiving scan data "comprising information collected from frames transmitted on the wireless network, wherein the received scan data is received from a wireless sensor configured to monitor the wireless network and collect information from frames transmitted on the wireless network." Sharma *et al.* and Heitman *et al.* also do not include identifying the relationship responsive to an analysis of the scan data and responsive to a relationship between the wireless sensor and a server.

Specifically, independent Claim 1 has been amended to recite:

1. A method for mapping the topology of a wireless network, the method comprising the steps of:

(a) receiving scan data ***comprising information collected from frames transmitted on the wireless network, wherein the received scan data is received from a wireless sensor configured to monitor the wireless network and collect information from frames transmitted on the wireless network, wherein the scan data is associated with monitoring of one or more wireless access points, one*** or more wireless network nodes or combinations thereof;

(b) identifying a relationship (1) between at least one of the wireless access points and at least one of the wireless network nodes or (2) between any two wireless network nodes based on the received scan data, a characteristic of at least one of the wireless access points, a characteristic of at least one of the wireless network nodes or combinations thereof***, wherein the relationship is identified responsive to an analysis of the scan data and responsive to a relationship between the wireless sensor and a server***; and

(c) storing the identified relationship, access point characteristic, node characteristic or combinations thereof in a system data store as topology data.

With regards to Claims 2-32, these Claims depend ultimately from Claim 1. Accordingly, the amendments and remarks with regard to Claim 1 apply with equal force here.

With regard to Claim 14, Sharma *et al.* and Heitman *et al.* do not teach the system data store storing topology data for each repetition and detecting potential security through a comparison of topology data from one repetition to another repetition. Applicant has amended Claim 14 to include these limitations.

With regard to Claim 29, Sharma *et al.* and Heitman *et al.* do not teach graphically represented characteristics or relationships as disclosed by Applicant. Specifically, graphically represented characteristics or relationships include whether a wireless access point of the one or more wireless access points is authorized, unauthorized, or ignored and whether a wireless network node of the one or more wireless network nodes is authorized, unauthorized, unassociated, an adhoc station, or ignored. Applicant has amended Claim 29 to further clarify these limitations.

With regard to Claim 33, Applicant has amended Claim 33 in a similar manner as Claim 1 including a wireless sensor configured to collect information from frames transmitted on the wireless network. Sharma *et al.* and Heitman *et al.* do not teach a wireless sensor for collecting information from frames. Further, Sharma *et al.* and Heitman *et al.* do not teach generating topology data by identifying a characteristic of the wireless sensor and relationships between the wireless sensor, node and access points. Additionally, Claim 33 has been amended to include topology comparison means for comparing topology data to prior topology data to evaluate potential security and policy violations of the wireless network. Sharma *et al.* and Heitman *et al.* do not teach utilizing topology for security and policy violation evaluation on wireless networks.

Specifically, independent Claim 33 has been amended to recite:

> 33. A system for mapping the topology of a wireless network, the system comprising:
>
> (a) storage means for storing topology data comprising access point characteristic data, wireless network node characteristic data, ***access point to node*** relationship data, ***node to node*** relationship data or combinations thereof;
>
> (b) ***a wireless sensor*** for scanning wireless transmissions within a wireless network and generating scan data therefrom***, wherein the scan data comprises information collected from frames transmitted on the wireless network***;
>
> (c) receiving means for receiving scan data from the ***wireless sensor over one of a wireless and wired connection***;
>
> (d) analysis means for generating topology data by identifying from scan data received by the receiving means a characteristic of a wireless network node, a characteristic of an access point, ***a characteristic of the wireless sensor,*** an ***access point to node*** relationship, a ***node to node*** relationship***, an access point to sensor relationship, a node to sensor relationship,*** or combinations thereof and for storing the generated topology data in the storage means;
>
> (e) output means for formatting topology data generated by the analysis means based upon a desired output format and for transmitting the formatted topology data to a desired output device***; and***
>
> ***(f) topology comparison means for comparing topology data to prior topology data to evaluate potential security and policy violations of the wireless network.***

With regards to Claims 34-35, these Claims depend from Claim 33. Accordingly, the amendments and remarks with regard to Claim 33 apply with equal force here. Additionally, Applicant has amended both Claims 34-35 to include intrusion detection means for detecting a usage volume anomaly, a connectivity pattern anomaly, a policy violation, a security violation or combinations thereof, and the mapping request is responsive to a trigger from the intrusion detection means. Applicant respectfully notes that Sharma *et al.* and Heitman *et al.* do not teach intrusion detection means for triggering mapping requests.

With regard to Claim 36, Applicant has amended Claim 36 in a similar manner as Claim 1 including a wireless sensor configured to perform the at least one scan to monitor the wireless network and collect information from frames transmitted. Also, the relationship between nodes is identified through analysis of the scan data and through a relationship between the wireless sensor and a server. Sharma *et al.* and Heitman *et al.* do not teach a wireless sensor for collecting information from frames and analysis of scan data for identifying relationships.

Specifically, independent Claim 36 has been amended to recite:

> 36. A system for mapping the topology of a wireless network, the system comprising:
>
> (a) a system data store (SDS) capable of storing topology data comprising access point characteristic data, wireless network node characteristic data, ***access point to node*** relationship data, ***node to node*** relationship data or combinations thereof; and
>
> (b) a system processor comprising one or more processing elements, wherein the system processor is in communication with the SDS and wherein the one or more processing elements are programmed or adapted at least to:
>
> (1) initiate at least one scan of one or more wireless access points, one or more wireless network nodes or combinations thereof***, wherein the at least one scan is performed by a wireless sensor configured to monitor the wireless network and collect information from frames transmitted on the wireless network***;
>
> (2) receive scan data ***comprising information collected from frames transmitted on the wireless network, and wherein the scan data is***

> associated with monitoring of one or more wireless access points, one or more wireless network nodes or combinations thereof;
>
> (3) identify a relationship (i) between at least one of the wireless access points and at least one of the wireless network nodes or (ii) between any two wireless network nodes based on the received scan data, a characteristic of at least one of the wireless access points, a characteristic of at least one of the wireless network nodes or combinations thereof, ***wherein the relationship is identified responsive to an analysis of the scan data and responsive to a relationship between the wireless sensor and a server***;
>
> (4) store the identified relationship, access point characteristic, node characteristic or combinations thereof in the SDS as topology data; and
>
> (5) format topology data generated based upon a desired output format; and
>
> (6) output the formatted topology data to a desired output device.

With regard to Claim 37, this Claim depends from Claim 36. Accordingly, the amendments and remarks with regard to Claim 36 apply with equal force here. Additionally, Applicant has amended Claim 37 to include an intrusion detection engine for detecting a usage volume anomaly, a connectivity pattern anomaly, a policy violation, a security violation or combinations thereof. Also, a limitation is added to initiate an iteration responsive to the intrusion detection engine detecting a violation. Applicant respectfully notes that Sharma *et al.* and Heitman *et al.* do not teach an intrusion detection engine for triggering iterations.

With regard to Claim 38, Applicant has amended Claim 38 in a similar manner as Claims 1 and 33 including a wireless sensor configured to perform the scan to monitor the wireless network and collect information from frames transmitted. The relationship between nodes is identified through analysis of the scan data. Also, a comparing step is included to compare topology data to prior topology data to evaluate potential security and policy violations of the wireless network. Sharma *et al.* and Heitman *et al.* do not teach a wireless sensor for collecting information from frames, analysis of scan data for identifying relationships, and comparing topology data for evaluation security and policy violations.

Specifically, independent Claim 38 has been amended to recite:

> 38. One or more computer-readable media storing instructions that upon execution by a system processor cause the system processor to map the topology of a wireless network by performing at least the steps comprising of:
>
> (a) initiating a scan of one or more wireless access points, one or more wireless network nodes or combinations thereof***, wherein the scan is performed by a wireless sensor configured to monitor the wireless network and collect information from frames transmitted on the wireless network***;
>
> (b) receiving scan data ***comprising information collected from frames transmitted on the wireless network, wherein the scan data is*** associated with monitoring of one or more wireless access points, one or more wireless network nodes or combinations thereof;
>
> (c) identifying a relationship (i) between at least one of the wireless access points and at least one of the wireless network nodes or (ii) between any two wireless network nodes based on the received scan data, a characteristic of at least one of the wireless access points, a characteristic of at least one of the wireless network nodes or combinations thereof***, wherein the relationship is identified responsive to an analysis of the scan data and responsive to a relationship between the wireless sensor and a server***;
>
> (d) storing the identified relationship, access point characteristic, node characteristic or combinations thereof as topology data; and
>
> (e) formatting topology data generated based upon a desired output format; ~~and~~
>
> (f) outputting the formatted topology data to a desired output device***; and***
>
> ***(g) comparing the topology data to prior topology data to evaluate potential security and policy violations of the wireless network, wherein the comparing comprises one of a rules-based comparison, a pattern matching-based comparison, and a combination thereof***.

Accordingly, Applicant respectfully submits that the rejection of Claims 1-38 as being unpatentable over Sharma *et al.* in view of Heitman *et al.* has been traversed, and respectfully requests withdrawal of this rejection.

CONCLUSION

Applicant would like to thank Examiner for the attention and consideration accorded the present Application. Should Examiner determine that any further action is necessary to place the Application in condition for allowance, Examiner is encouraged to contact undersigned Counsel at the telephone number, facsimile number, address, or email address provided below. It is not believed that any fees for additional claims, extensions of time, or the like are required beyond those that may otherwise be indicated in the documents accompanying this paper. However, if such additional fees are required, Examiner is encouraged to notify undersigned Counsel at Examiner's earliest convenience.

Respectfully submitted,

Date: December 10, 2007

/s/ Lawrence A. Baratta Jr. /
Lawrence A. Baratta Jr.
Registration No.: 59,553

Christopher L. Bernard
Registration No.: 48,234

Attorneys for Applicant

CLEMENTS | WALKER
1901 Roxborough Road, Suite 300
Charlotte, North Carolina 28211 USA
Telephone: 704.366.6642
Facsimile: 704.366.9744
lbaratta@worldpatents.com